I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

CARLA SCHERR*

You Better Watch Out, You Better Not Frown, New Video Surveillance Techniques are Already in Town (and Other Public Spaces)

Abstract: The use of video surveillance systems to capture images of Americans in public and pseudo-public spaces has grown faster than privacy law's ability to respond. New technologies and security concerns have revolutionized the way video surveillance images are captured, stored, and transmitted, and raise arguments that the subjects of such monitoring should have some right to control the use of those images. Because the monitored spaces are public, existing privacy law neither protects persons under surveillance nor acknowledges a need for such protection; therefore, the existing factors used to assess the reasonableness of an expectation of privacy are not appropriate to the new technologies. New factors should be developed in response to the capabilities of the new technologies, so that privacy laws addressing these technologies are thoroughly evaluated. These factors should include: (1) the distance between the camera and the subject, and the degree of magnification employed; (2) whether individual subjects are selected, tracked, or identified; (3) the durability and distribution of the images; (4) the likelihood of unauthorized image use and modification; and (5) the correlation of images with data from other sources.

---

*Carla Scherr is a Juris Doctor candidate at The Ohio State University Michael E. Moritz College of Law, class of 2008. She received a B.A. in Mathematics from Wellesley College in 1984 and a B.S. in Earth, Atmospheric and Planetary Sciences from the Massachusetts Institute of Technology in 1985. I thank my children for their extraordinary patience while I worked on this note, and I thank my husband for keeping a roof over my head and making it possible for me to enjoy a three-year sabbatical from real life.

I. INTRODUCTION

Privacy laws that address surveillance through the capture of visual images have traditionally relied on an analogy between actions visible to passers-by and actions captured by cameras. New surveillance technologies have rendered this analogy inapplicable; there is a difference between a passer-by and a video surveillance camera. A passer-by's observation is restricted to what can be seen by the naked eye. The passer-by can, of course, use vision-enhancing equipment, such as binoculars, but since the passer-by exists in the same time and space as the subject, the subject is likely to know of the observation and to have an opportunity to react. The subject of video surveillance, however, is not likely to know that he or she is being watched, what type of image is being captured, who is reviewing the image and where he or she is located, when the image is being reviewed, or how the image is being modified.

The past few years have seen tremendous advances in video surveillance technologies, as well as drastic decreases in the cost of those technologies. As a result, there has been an explosion in the use of video surveillance. At the same time, we have seen unprecedented changes in our society's security situation and attitudes towards privacy and public spaces. What we have not seen is corresponding changes in the privacy laws concerning video surveillance of public spaces.

Neither the Constitution nor the Bill of Rights specifically mentions a right to privacy. As a result, the conditions under which a person has a legitimate right to privacy are defined in much the same way as pornography, by using the "I'll know it if I see it" sniff test. Video surveillance of public spaces avoids all of the traditional tests used to establish a legitimate expectation of privacy. Thus, there is no legal tripwire to protect citizens from unwanted video image capture by either state or private actors. There is a gut feeling, nevertheless, that some right to control the use of one's image exists, even if the image was captured in a public space.

Until recently, society had neither the technology nor the desire to engage in detailed, wholesale, visual surveillance of its public spaces. After the terrorist attacks of 9/11, however, our technology and awareness of security issues matured quickly. We are now blessed, or perhaps cursed, with both the ability and the desire to watch and record the actions of our fellow citizens at an unprecedented level of detail that raises new privacy issues and compels us to re-examine our

expectations of privacy in the context of video surveillance of public spaces. The definition of a legitimate expectation of privacy, like the definition of pornography, must keep pace with changes in society and technology.

This note identifies factors that should be considered in assessing the adequacy of existing privacy law as applied to video surveillance of public spaces by private entities. The note restricts its consideration to situations where there is neither audio capture nor suspicious behavior by the subjects of the surveillance. Part II discusses recent developments in technology and society that postdate the establishment of the current legal framework. Part III provides an overview of the current legal framework. Part IV identifies factors arising from the new technologies and conditions that should be considered when privacy laws are modified to account for the ever-growing capabilities of our surveillance technology.

II. CHANGING TECHNOLOGIES AND THE CHANGING NATURE OF SURVEILLANCE

The current privacy-in-public standard was developed in the context of unsophisticated visual observation techniques and image-recording equipment with little capability to enhance the abilities of the naked eye. When the current law was developed, a person in a public space could expect to be seen and watched by others, and just as quickly forgotten. The technology and public interest of the time did not encourage the wholesale capture, storage, transmission, and manipulation of visual images, as is common today. Times have changed. The sheer number of cameras monitoring public spaces today makes it difficult to go into public without exposing oneself to continuous and permanent image capture. Few of our actions in public spaces are protected from visual surveillance by current privacy law, either under the search and seizure protections of the Fourth Amendment or current tort law provisions.

A. BETTER EQUIPMENT

It is difficult to imagine using pinhole-camera technology in a red-light camera system. Camera technology from just a few years ago would not have provided the image quality necessary for even the most mundane of today's surveillance applications. The ready availability of smaller, better, and cheaper cameras and video recorders requires society to address the legal and ethical aspects of capturing and storing images of unwilling or unknowing subjects.

The sophisticated digital surveillance cameras that are now available to the public at affordable prices[1] have democratized the ability to capture high-quality surveillance images. These cameras have amazingly high resolutions, 360° ranges of vision, and incredible zoom and night-vision capabilities.[2] Even more important than the revolution in image capture is the revolution in computing and data-storage technologies. For example, one generation ago, a computer's entire storage capacity was smaller than today's individual files; a few years ago, the storage capacity of an 8GB iPod nano,[3] which can be easily slipped into a pocket and forgotten, was unimaginable; and a few months ago, we could only dream that a TiVO digital video recorder capable of storing eighty hours of television would be the entry-level model available for less than $100.[4] Increases in computing speed and storage capacities, along with decreases in hardware size, have been critical to the development of surveillance technology. Without these technological advances, cameras and computers would be too big for surveillance purposes, capturing and processing digital images would be too slow to be useful, and the memory needed to store the images digitally would require warehouses full of memory units.

---

[1] 123 CCTV, Exterior Security Cameras, http://www.123cctv.com (last visited Jan. 29, 2008). Simple analog surveillance cameras are available for less than $50. A mini-dome camera with color, audio, 360 degrees of rotation and an infrared capability that allows images to be captured in almost complete darkness costs under $150. The wireless version costs just a little more. At the high end, an exterior pan, tilt, and zoom (PTZ) camera with a 23x optical zoom and 10x digital zoom (230x overall zoom) that can be controlled by a remote operator is available for less than $1500. *See also* CCTV Online Store, http://www.cctvonlinestore.com/ (last visited Jan. 29, 2008); PalmVid, Security Camera Systems, http://www.palmvid.com/ (last visited Jan. 29, 2008); CCTVFactory.com, Factory Prices on CCTV Camera Systems, http://www.cctvfactory.com/ (last visited Jan. 29, 2008) (examples of the plethora of websites where CCTV equipment can be bought); Extreme Surveillance, http://www.extremesurveillance.com (last visited Jan. 29, 2008) (information about integrated surveillance systems available to commercial, government, and residential customers).

[2] *See* Exterior Security Cameras, CCTV Online Store, Security Camera Systems, Factory Prices on CCTV Camera Systems, Extreme Surveillance, *supra* note 1.

[3] Apple, Apple–iPod nano–Technical Specifications, http://www.apple.com/ipodnano/specs.html (last visited Jan. 29, 2008).

[4] TiVo, Buy TiVo, https://www3.tivo.com/store/boxdetails.do?boxName=80hourseries2dt&boxsku=R64980 (last visited Jan. 29, 2008).

B. MORE EQUIPMENT

We are quickly establishing a Panopticon[5] in our cities by saturating them with surveillance cameras.[6] Cameras are everywhere and many of them are web-enabled. Great Britain is on the leading edge of the curve with approximately 4.2 million Closed-Circuit Television ("CCTV") cameras.[7] In the course of one day, a person in Britain can reasonably expect to be viewed by over 300 cameras.[8] Britain is also integrating its CCTV system with a national Automatic Number Plate Recognition system ("ANPR"),[9] which will be able to read 35 million license plates per day, increasing to 50 million reads per day by 2008.[10]

New York City is doing its best to keep up with Britain, but comes in a distant second with only 10,000 cameras installed.[11] Not everyone in New York is happy with even this level of surveillance. The Institute for Applied Autonomy has published a map of surveillance

---

[5] A famous example of behavior control through surveillance is the Panopticon, which was developed by 18th century philosopher Jeremy Bentham as the ideal, utilitarian prison. JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovic ed., Verso 1995), *available at* http://cartome.org/panopticon2.htm (last visited Jan. 29, 2008); Observing Surveillance, http://www.observingsurveillance.org/introduction.html (last visited Jan. 29, 2008). (The theory is to arrange the prisoners' cells in a circle around a central guard tower so that the guards can see inside every cell. This allows many prisoners to be monitored by few guards. Window blinds in the guard tower can be adjusted so that the guards can see out, but the prisoners cannot see in. Once the prisoners believe that the guards are watching them, it is not important whether the guards are actually watching or even present; the mere belief that the guards are present is sufficient to keep the prisoners from misbehaving. Thus, observation, or the appearance of observation, is a means of controlling behavior.).

[6] *See* Blog Toplist.com, Global CCTV Hub–Blog Toplist, http://www.blogtoplist.com/technology/blogdetails-8105.html (last visited Jan. 29, 2008) (discussion on camera surveillance systems and their use).

[7] SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY 19 (David M. Wood ed., 2006), http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf.

[8] *Id.*

[9] *Id.* at 19–20.

[10] *Id.* at 20.

[11] Erin Blakeley & Rodrigo Campos, *Feel Like You're Being Watched? You Are.*, NYC24, http://www.nyc24.org/2006/issue3/story01/index.html (last visited Jan. 29, 2008).

camera locations so that people can avoid them.[12] The Surveillance Camera Players, a pro-privacy organization, conducts weekend tours of heavily monitored areas of the city, pointing out the cameras.[13] Ironically, these tours have turned the cameras into a tourist attraction and are listed by Budget Travel Online as a recommended way to see New York.[14]

Public agencies are not the only entities increasing their use of real-time surveillance images; every city in America now has its share of private surveillance cameras that monitor public areas such as sidewalks, parking lots, freeways, and traffic lights. So many of these cameras are integrated with the Internet that any private citizen with a computer and an Internet connection can observe real-time video of people in public places around the world. Our computers have become a window through which we can watch ordinary citizens in such places as Caen, France, as they go about their daily commute,[15] golfers in Hawaii as they start their rounds at the Mauna Lani Resort,[16] weather conditions at the NOAA Amundsen-Scott South Pole Station,[17] or even the activities of penguins in Antarctica.[18] Thousands of web cams in every corner of the world distribute images of street scenes, famous landmarks, and even exhibits in zoos.[19] Some of the cameras

---

[12] Institute for Applied Autonomy, i-See, http://www.appliedautonomy.com/isee.html (last visited Jan. 29, 2008); New York Surveillance Camera Players, Map of Publicly Installed Surveillance Cameras in New York City, http://www.notbored.org/scp-maps.html (last visited Jan. 29, 2008).

[13] New York Surveillance Camera Players, Surveillance Camera Outdoor Walking Tours, http://www.notbored.org/scowt.html (last visited Jan. 29, 2008).

[14] Blakeley & Campos, *supra* note 11; Budget Travel, Contrarian Tours of Washington, D.C., New Orleans, Houston, and New York City, http://www.budgettravelonline.com/bt-dyn/content/article/2006/02/24/AR2006022401105.html (last visited Jan. 29, 2008).

[15] Caen.maville.com–webcam, http://www.caen.maville.com/vivre/webcam.php?IN_cam=Caen (last visited Jan. 29, 2008).

[16] Mauna Lani, Mauna Lani Resort Webcams, http://webcam.maunalani.com/webcamgolf.html (last visited Jan. 29, 2008).

[17] National Oceanic & Atmospheric Administration, South Pole Live Camera, http://www.cmdl.noaa.gov/obop/spo/livecamera.html (last visited Jan. 29, 2008).

[18] Martin Grund, Penguin Webcam–Antarctica, http://www.martingrund.de/pinguine/ (last visited Jan. 29, 2008).

[19] National Zoo, Animal Webcams at the National Zoo, http://nationalzoo.si.edu/Animals/WebCams/ (last visited Jan. 29, 2008).

allow the Internet observer to control who, what, and how closely the target subject is observed.[20] Indexes of real-time, or streaming, web cams exist on many websites, so finding real-time video is relatively easy.[21]

Permanently installed surveillance cameras are supplemented by omnipresent cell phone cameras, which collectively create "sousveillance" or a "reverse Panopticon" where the watched become the watchers.[22] Cell phone cameras can go where conventional cameras are excluded, for example, to Saddam Hussein's execution,[23] and can provide multiple viewpoints of the same item or event.

C. THE CHANGING NATURE OF SURVEILLANCE AND THE LOSS OF PRACTICAL OBSCURITY

Unlike the beat cop, automated video surveillance sees everything, forgets nothing, and never gets tired or distracted. It captures digital images that can be viewed at any time, from any place, as many times as desired, and can be modified and used well beyond the original intent of either the image collector or the subject. The extreme zoom

---

[20] PancakeCam, http://www.pancakecam.com/pancakecam.html (last visited Jan. 29, 2008); *see generally* EarthCam, Search Results for Interactive Webcam, http://search.earthcam.com/search/ft_search.php?s1=1&term=interactive+webcam&x=0&y=0, (last visited Jan. 29, 2008).

[21] Live Webcams, Free, Public Webcams Found Online, http://www.opentopia.com/hiddencam.php ("These webcams were found automatically through a variety of clever search techniques and update several times a day. Their owners may or may not have intended for them to be public, but they obviously are. Some of them are security cams in companies or semi-public places.") (last visited Jan. 29, 2008); Marcus' Live Streaming Video Cams, http://marcussharpe.com/vidstream.htm (305 streaming cams listed) (last visited Jan. 29, 2008); Web Cams Around the World, www.1000cam.com ("Over 10,000 cam from all over the Planet. 290 countries! 100% free viewing!") (last visited Jan. 29, 2008); EarthCam, Webcam Network, http://www.earthcam.com/company/aboutus.php (EarthCam–Where the World Watches the World®) ("EarthCam delivers real time live images of some of the world's most interesting and unique views and events. The portal offers the most extensive database allowing users to search by keyword or simply browse through the categories and subcategories.") (last visited Jan. 29, 2008).

[22] Steve Mann, James Fung & Raymond Lo, *Cyborglogging with Camera Phones: Steps toward Equiveillance*, http://www.eyetap.org/papers/docs/glogger.pdf (last visited Jan. 29, 2008) ("Sousveillance involves the recording of an activity by a participant in the activity. Usually involves a peer-to-peer approach that decentralizes observation to produce transparency in all directions.").

[23] *More Arrests Expected from Hussein Execution Video*, CNN.COM, Jan. 3, 2007, http://www.cnn.com/2007/WORLD/meast/01/03/saddam.execution/index.html.

capabilities of today's cameras allow them to be so distant from the subject that the subject is likely to be unaware and unsuspecting that surveillance might be present, and the camera can capture a subject's image at a level of intimacy that would be totally unacceptable if the image were observed in person.[24] Not even the cover of darkness provides protection; images can be captured in very low lighting and can capture information, such as the subject's temperature, that is not apparent to the naked eye.[25]

Even if the beat cop had walked around town with a video camera, the images taken would have enjoyed pseudo-privacy protection through "practical obscurity." The concept of "practical obscurity" applies to public information that is usually outside the public consciousness because it is contained in a large number of individual pieces that are practically impossible to accumulate and organize, or because it is impossible to find, for example a paper document stored in the dusty basement of the local courthouse[26] or in an infinitely large government warehouse.[27] One writer notes:

> [I]n the old days, it took time, talent and tenacity to find out anything. Enter electronic searchability, digital record-keeping and the Internet[,] . . . [n]ow even your inquisitive neighbor can ascertain how much you paid for your house, who loaned you the money, your finished square footage and perhaps even your floor plan—without leaving the comfort

---

[24] Comments of Deirdre Mulligan at the UnBlinking Symposium, Berkeley, Cal. (Nov. 3–4, 2006).

[25] FLIR Systems, What is Thermal Imaging? What is Infrared?, http://www.corebyindigo.com/applications/irprimer.cfm (last visited Jan. 29, 2008).

[26] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989) (information on a person's rap sheet exists in practical obscurity because its presence in the public record does not make it available for general use); Deveny v. Entropin, Inc., 139 Cal. App. 4th 408, 430 (Cal. Ct. App. 2006) (in a securities case, information posted on a website about a product's capabilities exists in practical obscurity and cannot be considered public information if the average investor would be unable to locate it without assistance).

[27] Tom Dirks, *Raiders of the Lost Ark (1981)*, GREATEST FILMS, http://www.filmsite.org/raid3.html (last visited Jan. 29, 2008) ("The Ark of the Covenant is crated in a wooden box and its lid is solidly nailed shut. Its stenciled label contains a long inventory number for identification: TOP SECRET, ARMY INTEL 9906753 DO NOT OPEN! A warehouseman pushes the crated Ark down a long aisle formed by huge stacks of similar crates in an enormous government warehouse, where it will again be hidden away–presumably by bureaucratic inefficiency.").

> of his own rather small cottage that he obviously paid too much for. (The reason I know this is because I looked it up on the county Web site.)[28]

The concept of practical obscurity applies to surveillance images, as well. Images that were once practically obscure because they were unavailable except as "hardcopies" now exist as digital data files and are stored in easily accessible databases. The posting of surveillance images on the Internet has lifted the veil of obscurity from public information and allowed it to be used in ways that were not anticipated when it was first defined as public. The issue surrounding practical obscurity is not simply whether public information should be public, but more practically, whether public information should always be easy to find and access. In some cases, the public is encouraged to watch and identify individuals or improper behavior.[29] Should such information be openly available on the Internet? Or should some sense of privacy be maintained by making access to the information more deliberate; for example, by requiring someone who wants access to the information to register online or go to the information's physical storage location?[30]

III. THE EXISTING LEGAL FRAMEWORK

Under the current laws, a person in a public space has no protection from unwanted video surveillance by either a state or private actor. The legal doctrines that protect persons from unwanted visual surveillance by state or private actors were developed under the basic premise that any person who goes into a public space has voluntarily waived any right to privacy to the extent of his or her person that is visible to passers-by. Given the abilities of new video surveillance technologies that enhance the naked eye, this basic assumption may no longer be valid.

---

[28] Rob Carrigan, *On the Web, 'Practical Obscurity' Has Practically Departed*, NEWSPAPERS & TECH., Jan. 2003, http://www.newsandtech.com/issues/2003/01-03/nt/01-03_carrigan.htm.

[29] *Texas Border Cam Test Catches 10 Illegal Immigrants*, CHICAGO SUN-TIMES, Jan. 8, 2007, at 49; *see also* Texas Border Watch Test Site, http://www.texasborderwatch.com/ (last visited Jan. 29, 2008); *Hundreds Turn in Marijuana Users in Boulder*, SUMMIT DAILY NEWS, Apr. 29, 2006, http://www.summitdaily.com/article/20060429/NEWS/60429001.

[30] *See* Arminda B. Bepko, *Public Availability or Practical Obscurity: The Debate Over Public Access to Court Records on the Internet*, 49 N.Y.L. SCH. L. REV. 967 (2004–05).

A. STATE ACTORS: PROTECTIONS UNDER THE CONSTITUTION AND FOURTH AMENDMENT

The "plain view" doctrine that developed under the Fourth Amendment search and seizure protections provides that state actors do not need a warrant to surveil activities and objects within plain view.[31] No reasonable expectation of privacy exists for persons or activities that can be observed by passers-by with the naked eye or with devices that reasonably resemble the naked eye. This includes situations in which the subject is in a public place,[32] the activity is a matter of public record,[33] or the subject voluntarily reveals the information to other people.[34]

However, this interpretation is not absolute. In *Katz v. United States*,[35] the Supreme Court recognized the right to privacy based on the expectation of the person being observed instead of the location being observed. Writing for the majority, Justice Stewart noted: "[t]he Fourth Amendment protects people not places."[36] Although *Katz* was

---

[31] United States v. Dunn, 480 U.S. 294, 305 (1987) (using a flashlight to see an item otherwise in plain view does not constitute a search); United States v. Barajas-Avalos, 377 F.3d 1040, 1056 (9th Cir. 2004), *cert. denied*, 543 U.S. 1188 (2005) (using a flashlight to look through a window into a darkened structure does not constitute a search); United States v. Lee, 274 U.S. 559, 563 (1927) (using a searchlight to view cases of illegal liquor on the deck of another vessel did not constitute a search).

[32] Rodriguez v. United States, 878 F. Supp. 20, 24 (S.D.N.Y. 1995) (video surveillance by federal agents did not violate the Fourth Amendment because the activity monitored occurred in a public place, specifically a public street where agents were hidden in a van); McCray v. State, 581 A.2d 45, 48 (Md. Ct. Spec. App. 1990) (videotapes of a defendant walking across a public street did not violate the Fourth Amendment because the defendant did not have a reasonable expectation of privacy under these circumstances).

[33] Hatch v. Town of Middletown, 311 F.3d 83, 91 (1st Cir. 2002) (the release of a child abuse arrest report did not violate the privacy of the subject of the arrest because the report was a public record) (Mr. Hatch was something of a celebrity due to participating in, and eventually winning, the first season of the reality game show *Survivor*).

[34] Willan v. Columbia County, 280 F.3d 1160, 1162 (7th Cir. 2002) (the disclosure of a candidate's past conviction for felony burglary by law-enforcement officers did not violate the candidate's right to privacy because he voluntarily attracted attention to his past by running for public office).

[35] Katz v. United States, 389 U.S. 347, 352–53 (1967) (the subject created a reasonable expectation of privacy for his conversation by going inside a phone booth and closing the door).

[36] *Id.* at 351.

a wiretapping case, it is pertinent to visual surveillance because it allows a person under surveillance to demonstrate his or her expectation of privacy by acting in a manner that would preserve privacy in most situations, such as by wearing a hat or facial disguise. Since *Katz* was decided, courts generally recognize that a reasonable expectation of privacy depends upon several conditions: what level of privacy is expected by the person being watched,[37] how does the observer behave and what surveillance techniques does he or she use,[38] and has the person being watched, or anyone with that person, consented to the surveillance.[39]

The "plain view" doctrine applies even when the passer-by must expend some extra effort to observe the person or activity,[40] such as providing artificial lighting to see objects in the dark.[41] Generally, the more sophisticated and unusual the equipment used by the observer, the less likely the courts will find the surveillance constitutional without a search warrant.[42] For example, using binoculars and other vision-enhancing equipment does not violate the subject's right to privacy, provided that the observation would be allowed if made

---

[37] Bond v. United States, 529 U.S. 334, 338–39 (2000) (a bus passenger may reasonably expect that his baggage will be handled, but it is not reasonable to expect that it will be "felt in an exploratory manner").

[38] United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (defendant had a reasonable expectation to be free from video surveillance by a camera mounted atop a power pole overlooking defendant's 10-foot-high fence).

[39] United States v. Nerber, 222 F.3d 597, 600 (9th Cir. 2000) (defendants had no reasonable expectation of privacy from secret video surveillance of their hotel room conducted while police informants were present, but did have a legitimate expectation of privacy once police informants had left and they were alone in their hotel room).

[40] Florida v. Riley, 488 U.S. 445, 450–52 (1989) (no warrant needed to observe a backyard greenhouse from a helicopter); Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (no warrant needed to photograph an industrial plant from navigable airspace); United States v. Gori, 230 F.3d 44, 52 (2d Cir. 2000) (no warrant needed to look through a door opened to accept a food delivery).

[41] Texas v. Brown, 460 U.S. 730, 739–40 (1983) (plurality opinion) (using a light to see items in a darkened car that were otherwise in plain view did not constitute a search).

[42] Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that thermal imaging a home's exterior to determine if the temperature was consistent with the growing of marijuana inside the house requires a warrant, because the technology used was not commonplace; privacy could be eroded by advances in police technology).

without binoculars.[43] Likewise, the subject has a greater expectation of privacy based on the extent and sophistication of the methods he or she uses to protect the activities from prying eyes.[44]

Even though the exterior of a private space is generally considered to be within the public sphere, the courts have considered the nature of the observation technology used when determining whether a warrant is needed.[45] Visual surveillance of the inside of a private space is even allowed without a warrant, although the resident's efforts, or lack thereof, to maintain privacy of the space are relevant.[46]

There is no safety in numbers. If more than one person is observed, a reasonable expectation of privacy is waived by the consent of one of the subjects, even if a warrant for surveillance would otherwise be required and the other persons being observed did not know about the surveillance.[47]

B. PRIVATE ACTORS: PROTECTIONS UNDER TORT LAW

When private parties undertake video surveillance of public spaces, neither the Fourth Amendment nor any other provisions of the

---

[43] United States v. Taborda, 635 F.2d 131, 139 (2d Cir. 1980) (using binoculars to observe the inside of a home is allowed without a warrant if the activities observed are visible from outside without the use of enhancement devices, because the householder has indicated a lack of subjective expectation of privacy by locating the activities where they can be seen from outside).

[44] *Cuevas-Sanchez*, 821 F.2d at 251 (a fence does not guarantee a reasonable expectation of privacy, but it does protect against casual observers); California v. Ciraolo, 476 U.S. 207, 214–15 (1986) (a fence does not establish a reasonable expectation of privacy from observers in the public airways because the backyard was visible to the naked eye of the observers).

[45] *Kyllo*, 533 U.S. at 34 (holding that thermal imaging a home's exterior to determine if the temperature was consistent with the growing of marijuana inside the house requires a warrant if obtaining information that could not otherwise have been obtained without a warrant).

[46] People v. Hicks, 364 N.E.2d 440, 444 (1st Dist. Ill. 1977) (failing to draw one's curtains demonstrates a lack of reasonable expectation of privacy); State v. Ward, 617 P.2d 568, 572–73 (Haw. 1980) (failing to draw one's curtains does not necessarily demonstrate a lack of reasonable expectation of privacy in cases where the windows were physically located where no naked-eye observer could see into them); Wheeler v. State, 659 S.W.2d 381, 390 (Tex. Crim. App. 1982), *reh'g granted*, 617 P.2d 381 at 388 (Tex. Crim. App. 1983) (a month-long stake-out to view the inside of a greenhouse through a five-inch gap in exhaust-fan louvers was a sustained and concerted attempt to penetrate the owner's many efforts to ensure the privacy of the greenhouse and violated the owner's reasonable expectation of privacy).

[47] *Nerber*, 222 F.3d at 604.

Constitution are implicated.[48] Many states have a constitutionally guaranteed right to privacy from search and seizure by government actors; fewer states address the issue of privacy in general.[49] For example, New York law addresses secret video surveillance, but only when performed by a law enforcement agency.[50] In Arizona, it is unlawful to videotape persons without their permission, but the law is qualified so that it applies only when the person being observed has a reasonable expectation of privacy and it exempts surveillance of private spaces, e.g., department store dressing rooms, when performed for security purposes.[51]

State tort laws provide possible alternative causes of action, including defamation, nuisance, humiliation, trespass, intentional infliction of emotional distress, assault, and breach of contract, as well as infringement of trademark, trade name or copyright, and restitution for unjust enrichment.[52] These laws are not particularly useful unless the surveillance images capture activity that is clearly private, or the images are used in a way that harms the subject or for commercial gain.

Surveillors also have rights. A citizen's right to use a video camera in a public place is protected by the Constitution, subject to restriction only by statute.[53] Using a camera is generally a lawful act and taking motion pictures is a reasonable means of securing evidence for trial.[54] Photographing a person in a private place without the

---

[48] State v. Diaz, 706 A.2d 264, 265 n.1 (N.J. Super. Ct. App. Div. 1998) (installing a video surveillance system in one's own home found not to implicate the federal or state constitutions because it is done by private individuals and not by the government); Commonwealth v. Kean, 556 A.2d 374, 378 (Pa. Super. Ct. 1989) (breaking into another person's home to install a hidden video camera did not implicate the federal or state constitutions because it was done by private individuals and not by the government).

[49] ALASKA CONST., art. I, § 22 (2007); MONT. CONST., art. II, § 10 (2005) (examples of state constitutions that have a right to privacy in general).

[50] N.Y. CRIM. PROC. LAW ch. 11-A, pt. 3, tit. T, art. 700 (McKinney 2007).

[51] ARIZ. REV. STAT. ANN. § 13-3019 (2007).

[52] Jeffrey F. Ghent, *Waiver or Loss of Right to Privacy*, 57 A.L.R.3d 16 § 2b.

[53] United States v. Gugel, 119 F. Supp. 897, 898 (E.D. Ky. 1954) ("The operation of a camera is a lawful act and a citizen's privilege to take pictures, unless made specifically unlawful by statute, is such a civil right as is protected by the Constitution of the United States.").

[54] Forster v. Manchester, 189 A.2d 147, 150 (Pa. 1963) (holding that a plaintiff's right to privacy was not invaded when motion pictures were taken of her by a private detective

subject's consent, however, is not within a citizen's rights, whether or not the photographer actually views the scene at the moment the photograph is taken.[55] Pictures taken in a public space where a person's activities can be observed by passers-by do not violate a person's right to privacy because the person exposed himself or herself to public observation, and, therefore, was not entitled to the same degree of privacy enjoyed within the confines of one's own home.[56] Photographs taken in a public area of a private facility that is open to all users of the facility do not violate the subject's right to privacy.[57]

C. FILLING THE GAPS: PRIVACY POLICIES

Public and private organizations have created policies that attempt to fill the voids left by federal and state laws. These organizations have identified the components of an ideal privacy policy and have implemented these components in various ways.[58] Examples of national, municipal, and industrial groups, as well as university privacy policies, are discussed in this section. Neither the policies nor the organizations included here are comprehensive; these examples are merely a sampling of the variety of privacy policies that have been created by private organizations.

---

working for the insurer of a driver with whom the plaintiff had been in an automobile accident).

[55] State v. Martin, 658 P.2d 1024, 1027 (Kan. 1983) (secretly photographing young women while they were changing clothes in an attic studio tended to uphold violation of eavesdropping statute which prohibited, inter alia, entering into a private place with intent "to observe the personal conduct of any other person or persons therein").

[56] *Forster*, 189 A.2d at 150.

[57] Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 483 (D. Me. 1987), *aff'd in part, and vacated in part*, 845 F.2d 347 (1st Cir. Me.) (photographing a passenger on cruise ship did not state cause of action for invasion of privacy; although photographers harassed passenger on several occasions, the harassment occurred in areas of ship open to all passengers).

[58] *See generally* THE CONSTITUTION PROJECT, GUIDELINES FOR PUBLIC VIDEO SURVEILLANCE (2007), *available at* http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation2.pdf (discussing the relevant issues and containing a section entitled Model Legislation for Establishing Public Video Surveillance Systems).

1. A NATIONAL POLICY: CCTV CODE OF PRACTICE

In 2000, the Information Commissioner of the United Kingdom issued the CCTV Code of Practice to assist CCTV system operators in understanding their legal obligations, to set out standards that must be followed to ensure compliance with the Data Protection Act of 1998, and to reassure the public about safeguards that should be in place.[59] The Code references eight data protection principles which were promulgated in the Data Protection Act of 1998.[60] These principles state that data must be relevant, limited, accurate, and secure; stored only as long as necessary; processed fairly and lawfully; and used for limited purposes in accordance with individuals' rights.[61] In support of these principles, the Code provides that the installation of a CCTV system should be undertaken only in accordance with the following standards:

- The system should fulfill a specific, defined purpose and should be installed only after the need for video cameras is assessed, the person or organization responsible for the operation is identified, and security and disclosure policies are established.[62]

- The location of the cameras, the times of day at which monitoring occurs, and the nature of specific image enhancement technologies used, e.g., infrared cameras, should be carefully considered to ensure that the system is used only as needed to fulfill the system's purpose.[63]

---

[59] INFO. COMM'R, CCTV CODE OF PRACTICE (2000), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cctv_code_of_practice.pdf. This document is being revised; a consultation draft of the 2007 revisions, entitled CCTV DATA PROTECTION CODE OF PRACTICE: CONSULTATION DRAFT is *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_cctv_consultation_draft_final.pdf.

[60] Data Protection Act, 1998, ch. 29 (Eng.), *available at* www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

[61] *Id.* pt. I, § 4.

[62] CCTV CODE OF PRACTICE, *supra* note 59, at 6.

[63] *Id.* at 7, 10.

- The quality and resolution of the images should be tailored to the purpose of the monitoring.[64] To help operators determine the level of image quality appropriate for their system, the proposed 2007 revision to the Code identifies four image-quality classifications: (1) sufficient to watch the flow of traffic or movement of a crowd without being able to detect individual figures; (2) sufficient to detect individual figures without being able to see individual faces; (3) sufficient to determine whether or not an individual is recognizable; and (4) sufficient to identify an individual with a degree of certainty that would allow the identification to be used in court.[65]

- The owners of any private spaces that are incidentally included in the captured images should be consulted, and the system operators should be trained to recognize the privacy implications of capturing images of private areas. Signs should be posted to inform the public that the space is being monitored.[66]

- A human operator should verify the results of automatic facial recognition processing.[67]

- Images should be retained in a secure location for no longer than necessary, accessible only by authorized personnel in a controlled location, and erased once the defined retention period has expired.[68]

---

[64] *Id.* at 9.

[65] CCTV DATA PROTECTION CODE OF PRACTICE: CONSULTATION DRAFT, *supra* note 59, at 8.

[66] CCTV CODE OF PRACTICE, *supra* note 59, at 7.

[67] *Id.* at 10.

[68] *Id.* at 11, 12.

- Requests from third parties to access stored images should be granted only in circumstances that are consistent with the purpose of the system and in accordance with documented disclosure policies.[69] Information concerning each release of stored images should be documented.[70]

- Subjects pictured in the images have a right to access the images in a timely fashion and without being charged an excessive fee.[71] Any person in the image, other than the person requesting to see the image, should be disguised or blurred.[72]

Once the decision has been made to implement a CCTV system, the Code is fairly comprehensive as it pertains to the use of surveillance images, but it presumes a right to collect images of unsuspecting persons in public spaces. Encouragingly, the proposed 2007 revision adds a caveat that was missing from the first version:

> CCTV is a privacy intrusive technology capable of putting a lot of law-abiding people under surveillance. You should carefully consider whether to use it; the fact that it is possible, affordable or has public support should not be the primary motivating factor. You should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals.[73]

2. A MUNICIPAL POLICY: THE DISTRICT OF COLUMBIA

The District of Columbia's Metropolitan Police Department ("MPDC") operates a growing system of CCTV cameras,[74] which it

---

[69] *Id.* at 13.

[70] *Id.* at 12.

[71] *Id.* at 15.

[72] *Id.* at 16.

[73] CCTV DATA PROTECTION CODE OF PRACTICE: CONSULTATION DRAFT, *supra* note 59, at 6.

[74] Press Release, District of Columbia Metropolitan Police Department, MPD Announces Planned Deployment of Last 19 CCTV Cameras to Help Combat Crime in DC Neighborhoods

alleges is "the most tightly regulated system of its kind in the nation."[75] The system is able to link with other public agency video networks, including those operated by the D.C. Public Schools and the District Department of Transportation. The department denies linking with privately operated camera networks and states that linking with the photo enforcement cameras it operates would be impossible due to incompatibilities between the different media used by each system.[76]

Highlights of the District's CCTV policies and procedures are posted on the Metropolitan Police Department's website, which also references the municipal code provisions in which the complete regulations are found.[77] According to the information posted on the website, the CCTV system is activated only during major events or emergencies, and only upon authorization of the Chief of Police or his designee.[78] All CCTV activities must be monitored by an MPDC official with the rank of lieutenant or above; under elevated threat-levels, supervision will be assumed by an assistant chief.[79] Camera operators must certify that they understand the policies and procedures and must not target or track individuals based on a classification that is legally protected.[80] Only public locations where there is "no reasonable expectation of privacy"[81] are targeted and areas monitored by permanent cameras are posted.[82] Cameras will not focus on printed

(June 25, 2007), http://newsroom.dc.gov/show.aspx/agency/mpdc/section/2/release/11365/year/2007/month/6. *See also*, Metropolitan Police Department, MPDC's Closed Circuit Television (CCTV) System, http://mpdc.dc.gov/mpdc/cwp/view,a,1238,q,541201,mpdcNav_GID,1545,mpdcNav,|31748|.asp (last visited Jan. 29, 2008). For an evaluation of the system, including photos of the control room, *see* U.S. GEN. ACCOUNTING OFFICE, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C., REP. NO. GAO-03-748 (2003), *available at* http://www.gao.gov/new.items/d03748.pdf.

[75] Metropolitan Police Department, CCTV–Policies and Procedures, http://mpdc.dc.gov/mpdc/cwp/view,A,1238,Q,541586.asp (last visited Jan. 29, 2008).

[76] Metropolitan Police Department, CCTV–Links with Other CCTV Systems, http://mpdc.dc.gov/mpdc/cwp/view,A,1238,Q,541579.asp (last visited Jan. 29, 2008).

[77] CCTV–Policies and Procedures, *supra* note 75.

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

materials, such as handbills or flyers, distributed or carried pursuant to the First Amendment.[83] Video images are recorded only with proper authorization and are deleted after ten days unless needed for potential litigation.[84]

3. AN INDUSTRY POLICY: IBM PRIVACY FACTORS

Researchers at the IBM T.J. Watson Research Center have identified six factors that should be addressed in a privacy policy.[85] Like the CCTV Code, the IBM factors provide that the data collected should be limited to that which is necessary to complete the task,[86] accessible only to authorized personnel,[87] and stored no longer than necessary in order to limit the nature and extent of the data usage.[88]

The IBM factors differ from the CCTV Code in a few areas. First, IBM acknowledges that the subjects' consent should be obtained.[89] If that is not possible, then signs should be posted to inform people using the space that it is under surveillance.[90] Second, the stored data should be encrypted or otherwise appropriately protected from misuse.[91] Third, authorization levels should distinguish between different needs for data access; for example, an "ordinary user" would have access to statistical information about the video, a "privileged user" would have access to limited individual information, and only law enforcement personnel would have access to the raw video and unlimited individual identity information.[92]

---

[83] *Id.*

[84] *Id.*

[85] Andrew Senior et al., *Enabling Video Privacy through Computer Vision*, IEEE SEC. & PRIVACY, May/June 2005, at 50.

[86] *Id.* at 52.

[87] *Id.*

[88] *Id.* at 53.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.* at 54.

As part of this discussion, the IBM researchers identified three levels of surveillance anonymity.[93] The first level preserves the most anonymity of the subjects, and is found in garden-variety CCTV systems that do not use zoom lenses or computer enhancement techniques.[94] The second level provides relative identification of the subjects. These systems recognize subjects for short periods of time, but they have no individual information about the subjects.[95] The third level, with the least anonymity, is provided by systems having the capability for absolute identification based on face-recognition or electronic ID swipes.[96] Third-level systems require the subjects to enroll in the system and can associate the subject with a database record of personal information.

Finally, consideration should be given to what enhancements should be stored with the video images, and whether privacy-invasive features should be masked.[97]

4. A UNIVERSITY POLICY: THE UNIVERSITY OF PENNSYLVANIA

The University of Pennsylvania Department of Public Safety has promulgated a video surveillance privacy policy that incorporates most of the factors addressed by IBM and the CCTV Code, and provides further standards regarding oversight and training.[98] The policy specifies the responsibilities of everyone involved in CCTV operations, and identifies the parties responsible for overseeing the daily operation of the system, keeping current with any changes in relevant law and security industry practices, and authorizing all CCTV monitoring.[99]

---

[93] *Id.* at 52.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *Id.* at 53.

[98] UNIV. OF PA., DIV. OF PUBLIC SAFETY, CLOSED CIRCUIT TELEVISION MONITORING AND RECORDING OF PUBLIC AREAS FOR SAFETY AND SECURITY PURPOSES, *available at* http://www.publicsafety.upenn.edu/downloads/Policy_CCTV_Monitoring_and_Recording.pdf (last visited Jan. 29, 2008).

[99] *Id.* at 2.

The policy establishes a CCTV Monitoring Panel to review the camera locations, requests for data access, and the policy itself. The panel is also ensuring that the group directly in charge of the program adheres to established policy and procedure.[100] The faculty, staff, students, university president, and the Safety and Security Committee are each represented on the panel.[101] Any member of the panel may audit monitoring operations, including videotape storage, at any time without prior notice.[102] The policy defines the procedure by which decisions by the panel can be appealed, including how to file a petition to forgo installation of a proposed camera or to request the removal of an existing camera.[103]

Personnel involved in video monitoring must be appropriately trained and continuously supervised.[104] Training must include technical, legal, and ethical parameters of appropriate camera use, as well as cultural awareness.[105] Operators must receive, understand, and acknowledge the CCTV policy.[106]

Data collection may be authorized for legitimate safety and security purposes only.[107] Collecting data for any purpose other than deterring crime and promoting campus safety is prohibited.[108] Data collection is limited to what is visible with unaided vision.[109] Surveillance of residential lounges and hallways is strictly forbidden unless the Vice President of Public Safety determines that a specific risk exists.[110] The surveillance system will not focus on people becoming intimate in public areas or look through windows to view private rooms or areas, nor will it target individuals based on race,

---

[100] *Id.*

[101] *Id.* at 3.

[102] *Id.* at 4.

[103] *Id.*

[104] *Id.* at 4.

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] *Id.* at 2.

[109] *Id.* at 4.

[110] *Id.* at 3.

gender, ethnicity, sexual orientation, disability, or any other classification protected by the University's non-discrimination policy.[111] Information gained in violation of the procedures will not be used in any disciplinary proceeding against faculty, staff, or students.[112]

The video surveillance policy and guidelines, and the locations and capabilities of CCTV cameras are published semi-annually in the campus newspaper and can be requested at any time.[113] The locations being monitored are appropriately posted.[114] The locations of temporary cameras for special events will be published before the event, if possible.[115]

CCTV monitoring centers must be configured to prevent tampering with or duplicating recorded information.[116] Information is to be used exclusively for security and law enforcement purposes, and will be released only when authorized by the Vice President of Public Safety according to procedures established in the policy.[117] Videotapes must be stored in a secure location accessible to authorized personnel only.[118] The release of videotapes requires the approval of the Monitoring Panel and the Vice President of Public Safety, except for videotapes directly related to criminal investigations.[119] Release will be approved only for legitimate purposes and requires at least five affirmative votes.[120]

---

[111] *Id.* at 2.

[112] *Id.*

[113] *Id.* at 3.

[114] *Id.* at 4.

[115] *Id.* at 3.

[116] *Id.* at 4.

[117] *Id.* at 2.

[118] *Id.* at 4.

[119] *Id.* at 3.

[120] *Id.* at 4.

IV. SURVEILLING THE FUTURE

Changes in video surveillance technologies, the amount of video surveillance images being captured in public spaces, and society's changing attitudes towards surveillance require us to reevaluate the factors used to measure the right to privacy from public video surveillance. The subject's ability to see the video surveillance camera; to anticipate the type of images being captured; to know who, how, where, and when the images will be used; and to control the use of personally identifiable information are important factors that should be considered. These factors inform fundamental questions concerning the right to know that one is under video surveillance, the existence of meaningful choices about participating in video surveillance, and the ability to control one's image data.

A. DISTANCE AND MAGNIFICATION

Privacy laws should consider the distance between the surveillance camera and the subject, and the level of magnification used. The distance between the camera and the subject is an important factor because the reach of today's technology allows surveillance systems to capture images of persons who are unaware they are being observed. Although the images captured are similar to what would be seen by a passer-by, the subject is not aware of the surveillance, and thus cannot choose to leave the area being surveilled or otherwise indicate an unwillingness to participate in the surveillance. Magnification allows the observer to see the subject, or parts of the subject, at a level of detail that is not normally visible to others. Unlike the distance issue, a passer-by in this case would not be able to see the same view as the video surveillance system unless the passer-by was permitted to be in intimate proximity to the subject. Again, the subject of the surveillance cannot rely on seeing the camera, the size of the lens, or the location of the person capturing the subject's image, to adequately judge the type of image being captured and respond appropriately.

B. IMAGE DURABILITY AND DISTRIBUTION

Privacy laws should consider how long a video surveillance image is kept and whether it is available to viewers far distant from the place where the image was captured. Unlike the beat cop, video surveillance images can be watched long after being captured and far removed from the place of capture. The subject of the image capture has no way of knowing how far away in time and space his or her images will

be seen, and, thus, has no way to judge whether to opt-out of participating.

C. SELECTING AND TRACKING THE SUBJECT

Privacy laws should consider the video surveillance system's ability to select and track individual subjects. Surveillance began as a means to track "shady characters" that were suspected of some wrongdoing. Slowly this changed, first as society installed video surveillance cameras at places with a high potential for criminal activity, such as ATMs, banks, and gas stations, and then as surveillance cameras began watching people who were not suspected of any wrongdoing and were not in places prone to crime. As the use of cameras that are controlled by human operators increases, the chance that operators will use their power inappropriately,[121] or that protected classes of people will be singled out for surveillance also increases.

> During my time in the control room, from 9 p.m. to midnight, I experienced firsthand a phenomenon that critics of CCTV surveillance have often described: when you put a group of bored, unsupervised men in front of live video screens and allow them to zoom in on whatever happens to catch their eyes, they tend to spend a fair amount of time leering at women . . . . In Hull, this temptation is magnified by the fact that part of the operators' job is to keep an eye on prostitutes. As it got late, though, there weren't enough prostitutes to keep us entertained, so we kept ourselves awake by scanning the streets in search of the purely consensual activities of boyfriends and girlfriends making out in cars . . . . [O]perators, in addition to focusing on attractive young women, tend to focus on young men, especially those with dark skin.[122]

---

[121] Notbored.org, Abuses of Surveillance Cameras, http://www.notbored.org/camera-abuses.html (last visited Jan. 29, 2008) (listing multiple instances of casino surveillance camera operators who turned the cameras into a "peep show" by targeting specific body parts of female gamblers and employees, and also police officers who misused surveillance cameras, among others).

[122] Jeffrey Rosen, *A Watchful State*, N.Y. TIMES, Oct. 7, 2001, http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html.

D. UNAUTHORIZED IMAGE USE AND MODIFICATION

Privacy laws should consider the nature and extent of any unauthorized use or modification of the captured image. The privacy implications of the misuse of human images was one of the frontiers boldly explored by Gene Roddenberry and the creators of the TV series "Star Trek: The Next Generation" ("TNG"). Two episodes of TNG specifically addressed the use and abuse of human images.[123]

In "Hollow Pursuits,"[124] Ensign Barclay creates holographic versions of the senior officers and uses them to play out his fantasies on the holodeck. In TNG, the holographic images are so lifelike that they are physically indistinguishable from the real people, but Barclay modifies the holograms so they are subservient to Barclay, totally unlike their real counterparts. When the senior officers find out about Barclay's activities they feel violated, both by the mere existence of the images and by the way their holographic selves have acted. One officer comments that although there is no rule against what Barclay did, "there should be."

In "Booby Trap,"[125] Geordi La Forge, the chief engineer, creates a holographic representation of Leah Brahms, the woman who designed the ship's engines, to obtain assistance during an engineering emergency. Unlike Ensign Barclay's creations in "Hollow Pursuits," the holographic image of Leah Brahms is extremely realistic because La Forge based it on her personnel file.[126] While working together on the engineering emergency, La Forge develops a personal relationship with the holographic Leah Brahms. When the real Leah Brahms comes aboard in a later episode,[127] La Forge treats her in a manner consistent with a prior relationship. Understandably, she finds his behavior overly familiar and entirely inappropriate, because for her,

---

[123] Paul Joseph & Sharon Carton, *The Law of the Federation: Images of Law, Lawyers, and the Legal System in "Star Trek: The Next Generation,"* 24 U. TOL. L. REV. 43, 80–83 (1992).

[124] StarTrek.com, Episode: Hollow Pursuits, http://www.startrek.com/startrek/view/series/TNG/episode/68444.html (last visited Jan. 29, 2008).

[125] StarTrek.com, Episode: Booby Trap, http://www.startrek.com/startrek/view/series/TNG/episode/68414.html (last visited Jan. 29, 2008).

[126] A discussion of the Federation's privacy laws and whether an engineering emergency is a valid reason for violating them will have to wait for another note. Further enlightenment about Federation law in general can be found at Joseph & Carton, *supra* note 123.

[127] StarTrek.com, Episode: Galaxy's Child, http://www.startrek.com/startrek/view/series/TNG/episode/68486.html (last visited Jan. 29, 2008).

this is their first meeting. For La Forge, however, they are close friends. When the real Leah Brahms finds out about the holographic Leah Brahms, she also feels violated by the way "she" has been used.

The Star Trek writers recognized that people want to control their images, regardless of whether the image is an accurate reflection of them or is modified to meet the possessor's needs. Although the technology used in TNG to use and misuse images is beyond our reach, the desire to "enhance" the images of others goes back as long as there have been images on which to draw mustaches.

In real life, the misuse of visual images is also a concern. Spencer Tunick is famous for photographing urban landscapes containing large numbers of nude people.[128] In March 2006, Tunick photographed approximately 1700 people in Newcastle, England. The photos were taken in an urban area populated with private surveillance cameras, many of which captured images of participants as they walked naked from the staging area to the location where the photograph was taken. It was discovered afterwards that the camera operators, including police department employees, had obtained stills of the nude people from the surveillance camera video and offered them for sale at the local bars and pubs, even at the subjects' regular drinking establishments.[129] The police department promised to investigate.[130]

Within this situation lies a deeper question of how to allocate the risk that video surveillance images will be misused. Since the person in possession of the video surveillance images is the only one who will know for certain whether the images exist, surely the possessor is in the best position to bear the burden of safeguarding the images.

---

[128] See examples of his work at I-20 Gallery, Selected Images by Spencer Tunick, http://www.i-20.com/artist.php?artist_id=19 (last visited Jan. 29, 2008).

[129] Hille Koskela, *(Re)exposing the Naked Body: The Misuse of Surveillance Cameras in Spencer Tunick's Photography Event*, UnBlinking: Symposium, Nov. 3–4, 2006, http://www.law.berkeley.edu/institutes/bclt/events/unblinking/unblinking/koskela-unblinking-abstract.htm; Oliver Duff, *Film of Artist's Mass Nude Photo Shoot Being Sold in Pubs*, THE INDEP. ONLINE EDITION, Mar. 21, 2006, http://news.independent.co.uk/uk/this_britain/article352607.ece.

[130] Duff, *supra* note 129.

E. VIDEO IMAGES ARE PERSONALLY IDENTIFIABLE INFORMATION

Video surveillance images are data and may contain personally identifiable information ("PII").[131] Therefore, these images should be subject to the same protections as other forms of personally identifiable information.

Like fingerprints and retina patterns, facial images captured by video surveillance systems are biometric information that can be used to uniquely identify individuals.[132] Facial images, when combined with location, place, and time information provided by the capturing surveillance camera, uniquely identify a person at a specific place and time. Face recognition technology allows absolute and relative identification of subjects. Absolute identification matches a face to a name; relative identification matches a face to a face. Face recognition technology searches through images to find all occurrences of a "tagged" facial image.[133] This can be used to find occurrences of the same face in situations where a name is provided, which could be devastating to the privacy of individuals whose facial images are captured at political rallies or abortion clinics. Even if the surveillance images are de-identified by randomly altering certain data fields, such as date and time, so that the information is no longer PII, it is possible

---

[131] PII is information that "identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, social security number, and credit card information. To the extent unique information (which by itself is not Personally Identifiable Information) such as a personal profile, unique identifier, biometric information, and IP address is associated with Personally Identifiable Information, then such unique information will also be considered Personally Identifiable Information . . . ." P3Pwriter, Privacy Definitions, http://www.p3pwriter.com/LRN_000.asp#PII (last visited Jan. 29, 2008).

[132] ELEC. FRONTIER FOUND., BIOMETRICS: WHO'S WATCHING YOU? (Sept. 2003), http://www.eff.org/wp/biometrics-whos-watching-you.

[133] Riya–Visual Search, http://www.riya.com/ (last visited Jan. 29, 2008) ("Find an item you like, and Like.com will show you items that are visually similar.") (supports searches for objects and people). *See also* Eigenfaces/Photobook Demo, http://vismod.media.mit.edu/vismod/demos/facerec/basic.html (last visited Jan. 29, 2008); Jacqui Cheng, *Facial Recognition Slipped into Google Image Search*, ARS TECHNICA, May 30, 2007, http://arstechnica.com/news.ars/post/20070530-facial-recognition-slipped-into-google-image-search.html ("While currently unofficial and unannounced, users can now search for images that only contain faces by appending a query string onto the end of a search URL.").

to re-identify the information if there are enough distinct pieces of de-identified data available or simply through clever technology.[134]

Under the current law, the right to distribute images of a subject belongs to the person who captured the images and not the subject. However, if the images are PII, then current privacy law supports the idea that the person whose data is captured, i.e., the subject of the surveillance, retains the right to control that data. In addition, other rules that apply to personal information, such as the Fair Information Practices Act of 1973,[135] would apply to facial images captured by video surveillance systems. An Internet-enabled video surveillance system that captures images of children might also be subject to the parental permission restrictions of the Children's Online Privacy Protection Act ("COPPA").

F. CORRELATING DATA FROM MULTIPLE SOURCES

Privacy laws should consider whether the surveillance image could be combined with information of other types or from different sources. For example, the District of Columbia Police Department has the ability to link its CCTV network with other public agency video networks, such as the traffic cameras operated by the Department of Transportation and the CCTV network operated by the D.C. Public Schools.[136] Likewise, the British CCTV system recently added

---

[134] *Interpol: Pedophile in Photo ID'd as Teacher*, MSNBC.COM, Oct. 16, 2007, http://www.msnbc.msn.com/id/21307230/.

[135] The Fair Information Practices Act of 1973 outlines basic principles of data usage:

1. There must be no personal data record-keeping systems whose very existence is secret;
2. There must be a way for an individual to find out what information is in his or her file and how the information is being used;
3. There must be a way for an individual to correct information in his or her records;
4. Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and
5. There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

Center for Democracy & Technology, Privacy Basics: HEW Code of Fair Information Practices, http://www.cdt.org/privacy/guide/basic/hew.html (last visited Jan. 29, 2008).

[136] CCTV – Links with Other CCTV Systems, *supra* note 76.

loudspeakers to its system to create "speaker cams" that can scold persons observed engaging in "anti-social behavior," such as littering.[137] New York City plans to network thousands of private and public video surveillance cameras, electronic license plate readers, and remote-controlled traffic barriers, controlled by a 24-hour command center.[138]

The same technological advances that make sophisticated surveillance systems possible also allow the collection of vast quantities of personal data, including credit card purchases, E-ZPass usage, car registration information, grocery store loyalty programs, library borrowing records, and any other records that are kept digitally.[139] "Dataveillance" is the term coined to describe the practice of automatically correlating one person's information from multiple sources.[140] For example, credit card gas purchases could be compared with purchases from auto service centers to estimate the number of miles driven since the last servicing. Based on this information, a reminder that servicing is needed could be sent to the vehicle owner. The same technique could be used to compare car registration information with insurance company records so that drivers without insurance could be flagged. Dataveillance by government entities has been called "the technological equivalent of a general warrant on the entire population," because everyone is presumed guilty until proven innocent.[141] It violates the privacy principle that personal information supplied for one purpose should not be used for another purpose without express consent from the individual concerned.[142]

The possibilities presented by dataveillance explode when data is combined with visual images. With dataveillance, the identity of the person or vehicle must often be inferred from usage of a credit card.

---

[137] Will Byrne, *Orwell Rolls in His Grave: Britain's Endemic Surveillance Cameras Talk Back,* THE RAW STORY, May 30, 2007, http://rawstory.com/printstory.php?story=6292.

[138] Alex Kingsbury, *Gotham's Sky Spies*, U.S. NEWS & WORLD REPORT, July 23, 2007, available at http://www.usnews.com/usnews/news/articles/070715/23cctv.htm.

[139] Posting of Bruce Schneier to Schneier on Security, The Future of Privacy, http://www.schneier.com/blog/archives/2006/03/the_future_of_p.html (Mar. 6, 2006, 05:41 PST).

[140] Australian Privacy Foundation, Australia as a Surveillance Society (Jun. 30, 1994), http://www.privacy.org.au/Papers/SubmnNSWParlt9406.html.

[141] *Id.*

[142] *Id.*

Surveillance videos capture uniquely identifying information, such as faces and license plates. With a license plate tracking system like the one being installed in Great Britain, it is possible to know not only how many miles were traveled, but also where the vehicle went. If a data collection and control system like GM's OnStar[143] were combined with information from municipal traffic light cameras, then it would be possible to create a system where the driver of a vehicle caught running red lights could be scolded by an OnStar operator who could then deactivate the car. In this scenario, Big Brother becomes "Mom cam."[144]

It is easy to imagine a time, not so far from now, when we will have the technology to aggregate surveillance cameras, biometric identification systems, and other discrete monitoring systems into a vast network of real-time surveillance. It will allow us to locate particular individuals anywhere at anytime, to know where they have been, where they are going, who they are with, who they are likely to meet, and even what the person has with them. Omniscient, omnipresent visual surveillance will certainly not be "the end of western civilization as we know it," but it will change the way we act. The question is not whether we will react, but what the nature and extent of the reaction will be, and what will be lost in the inevitable cat-and-mouse game between the observers and the observed.

V. CONCLUSION

Privacy is not a static, one-size-fits-all concept. New surveillance technologies and changing societal views towards information sharing constantly change the calculus of privacy law. The calculus only becomes more complex because new technologies and changing societal norms may work toward opposite ends; new technologies make video surveillance more intrusive and suggest the need to strengthen privacy laws, while changes in societal norms indicate more acceptance of sharing one's personal information and suggest that expectations of privacy are becoming weaker. Whichever direction these changes take us, it is clear that factors that were appropriate when the beat cop was responsible for the surveillance of public

---

[143] OnStar by GM, http://www.onstar.com (last visited Jan. 29, 2008).

[144] *See, e.g.*, *Stop Thief! GM's OnStar Could Stop Stolen Cars*, MSNBC.COM, http://www.msnbc.msn.com/id/21134540/vp/21206876#21206876 (video report) (last visited Jan. 29, 2008).

spaces should be reconsidered in light of new technologies used in the video surveillance of public spaces.